مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Akira Ransomware Threat

Tracking #:432316426

Date:23-10-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed the Akira ransomware operation has emerged as a prominent threat in the cyber landscape, characterized by its continual evolution and adaptability.

TECHNICAL DETAILS:

Akira ransomware has solidified its presence in the ransomware ecosystem, demonstrating significant adaptability and evolution in its tactics, techniques, and procedures (TTPs). Recent findings by Cisco Talos indicate a shift in Akira's strategy, oscillating between encryption and data exfiltration tactics while leveraging newly disclosed vulnerabilities for initial access.

Akira's Ransomware Evolution:

1. **Continuous Adaptation**: Akira has transitioned through various encryptor iterations, recently launching a Rust-based version for ESXi and a return to C++ for their Windows variant, indicating a strategic pivot towards stability and reliability.
2. **Data Exfiltration Focus**: In early 2024, Akira appeared to prioritize data exfiltration over encryption, likely as a temporary measure while retooling their encryptor. However, the recent resurgence of encryption tactics alongside data theft suggests a recalibration of their double-extortion model.
3. **Exploitation of Vulnerabilities**: Akira affiliates have exploited multiple critical vulnerabilities (CVEs) in network appliances and software, allowing rapid compromise and lateral movement within targeted environments. Key vulnerabilities include:
    - **CVE-2024-40766**: Remote code execution in SonicWall SonicOS.
    - **CVE-2020-3259 & CVE-2023-20263**: Arbitrary code execution vulnerabilities in Cisco ASA and Firepower Threat Defense.
    - **CVE-2023-48788**: Exploitation of vulnerable FortiClientEMS software.
    - **CVE-2023-27532**: Compromise of Veeam backup server to access encrypted credentials.
4. **Targeted Sectors**: The operation predominantly targets organizations within manufacturing and technical services, reflecting a strategic focus on high-impact sectors.

Attack Chain:

1. **Initial Access**: Akira affiliates utilize common vectors such as compromised VPN credentials and exploit newly disclosed CVEs to gain entry into networks.
2. **Privilege Escalation and Lateral Movement**: Once inside, they employ techniques such as credential harvesting via PowerShell scripts and utilize RDP connections for lateral movement, often disabling security tools to evade detection.
3. **Deployment of Ransomware**: Following successful infiltration and privilege escalation, Akira deploys ransomware to encrypt critical files while also exfiltrating sensitive data for extortion.
4. **Rapid Compromise Strategy**: Akira's approach emphasizes exploiting vulnerabilities in widely used network appliances to establish footholds and deploy ransomware swiftly, maximizing operational impact.

INDICATORS OF COMPROMISE(IOCs):

Attached in Excel File

RECOMMENDATIONS:

1. **Patch Management**: Regularly update and patch systems, particularly for network appliances and critical software, to mitigate the risk posed by known vulnerabilities. Immediate attention should be given to CVEs identified in Akira's recent attacks.
2. **Network Segmentation**: Implement strict network segmentation to limit lateral movement within the environment. This can help contain the spread of ransomware should a breach occur.
3. **Multi-Factor Authentication (MFA)**: Enforce MFA for all remote access solutions, including VPNs, to reduce the likelihood of unauthorized access through compromised credentials.
4. **Incident Response Planning**: Develop and regularly test an incident response plan that includes ransomware-specific scenarios. This should detail steps for isolating affected systems, communicating with stakeholders, and engaging law enforcement if necessary.
5. **User Education and Awareness**: Conduct regular training for employees on recognizing phishing attempts and other social engineering tactics commonly used by ransomware operators.
6. **Data Backup and Recovery**: Maintain regular backups of critical data and ensure that these backups are stored offline or in a manner that is inaccessible to ransomware. Regularly test the restore process to ensure data can be recovered quickly.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://blog.talosintelligence.com/akira-ransomware-continues-to-evolve/